WHAT IS CLAIMED IS:

Sub a1

1. A method of securing a token from unauthorized use, comprising the steps of:

receiving a first message transmitted from a host processing device and addressed to a PIN entry device according to a universal serial bus (USB) protocol;

accepting a PIN entered into the PIN entry device; and

transmitting a second message comprising at least a portion of the first message and the PIN from the PIN entry device to the token along a secure communication path.

2. The method of claim 1, wherein:

the first message is received in the PIN entry device; and

the second message is transmitted from the PIN entry device directly to the token along the secure communication path.

3. The method of claim 1, wherein:

the step of receiving the first message transmitted from a host processing device and addressed to a PIN entry device comprises the steps of:

receiving the first message in a USB-compliant hub communicatively coupled to the host processing device via a first communication path;

transmitting the first message to the PIN entry device communicatively coupled to the USB-compliant hub; and

the step of transmitting the second message comprising the portion of the first message and the PIN and at least a portion of the first message from the PIN entry device to the token along a secure communication path comprises the steps of:

transmitting a second message from the pin entry device via the USB hub.

4. The method of claim 3, wherein the step of transmitting the second message from the PIN entry device via the USB-compliant hub comprises the steps of:

transmitting a third message comprising the PIN from the PIN entry device to the USB-compliant hub;

processing the message in the USB-compliant hub to produce the second message; and

transmitting the second message from the USB-compliant hub.

5. The method of claim 1, wherein the signal received from the host processing device is generated in an API interface.

6. The method of claim 1, wherein:

the first message is encrypted according to a first encryption key; and

the pin entry device comprises a decryption module having access to the first encryption key for decoding the first message.

7. The method of claim 1, wherein the second message is transmitted to the token according to a USB-compliant protocol.

8. The method of claim 1, wherein the second message is encrypted according to a second encryption key and the token comprises a decryption module having access to the second encryption key.

9. The method of claim 1, wherein the step of transmitting the second message from the PIN entry device to the token further comprises the step of:

encrypting the second message according to a second encryption key stored in the PIN entry device and the token; and

transmitting the encrypted second message to the token.

10. The method of claim 1, wherein the first message is a message transmitted from the host processing device to authorize a transaction.

11. The method of claim 1, wherein the first message is a message transmitted from the host processing device to authenticate a user of the token.

12. An apparatus for securing a token from unauthorized use, comprising:

a PIN entry device, communicably coupleable to a host processing device transmitting a first message addressed to the PIN entry device, and communicatively coupleable to the token according to a universal serial bus USB protocol, the PIN entry device comprising:

a user input device, for accepting a user-input PIN; and

a processor, communicatively coupled to the user input device, the processor for receiving the first message and combining the first message with the user-input PIN, and for producing a second message having at least a portion of the first message and the user-input PIN.

13. The apparatus of claim 12, wherein the first message is encrypted according to a first encryption key and the PIN entry device further comprises:

a module for decrypting the first message from the host processing device according to a first encryption key.

14. The apparatus of claim 13, wherein the module is a software module having instructions stored in a memory accessible to the processor.

15. The apparatus of claim 14, wherein the PIN entry device further comprises:

a second module for encrypting the second message according to a second encryption key.

16. The apparatus of claim 15, wherein the second module is a software module having instructions stored in a memory accessible to the processor.

17. The apparatus of claim 12, wherein the PIN entry device further comprises an output device for prompting the user to enter the PIN.

18. A method for securing a token from unauthorized use, comprising:

intercepting a first message from the host processing device addressed to the token in a hub;

providing the intercepted message to a PIN entry device communicatively coupled to the hub;

accepting a second message from the PIN entry device comprising a user-entered PIN;

generating a third message from the second message, the third message comprising the user-entered pin and at least a portion of the first message; and

transmitting the third message from the USB-compliant hub to the token.

19. The method of claim 18, further comprising the step of:

encrypting the third message according to a first encryption key stored in a memory of the token before transmitting the third message to the token.

20. An apparatus for securing a token from unauthorized use, comprising:

a USB-compliant hub, communicably coupleable between a host processing device and the token, the USB compliant hub having;

means for intercepting a message addressed to the PIN entry device;

means for generating a third message from the first message and a user-entered PIN; and

means for transmitting the third message to the token;

a PIN entry device, communicatively coupled to USB-compliant hub, for accepting a user-entered PIN and providing the user-entered PIN to the USB-compliant hub.

21. The apparatus of claim 20, wherein the means for intercepting a message addressed to the PIN entry device, the means for generating the third message from the first message and a user-entered PIN and the means for transmitting the third message to the token comprises at least one processor having at least one communicatively coupled memory storing processor instructions for intercepting a message addressed to the PIN entry device, for generating the third message from the first message and a user-entered PIN, and for transmitting the third message to the token.

22. The apparatus of claim 20, wherein the USB-compliant hub further comprises a means for encrypting the third message according to an encryption key stored in a memory of the token.

23. The apparatus of claim 22, wherein the means for intercepting a message addressed to the PIN entry device, the means for generating the third message from the first message and a user-entered PIN, the means for encrypting the third message according to an encryption key stored in the memory of the token and the means for transmitting the third message to the token comprises at least one processor having at least one communicatively coupled memory storing processor instructions for intercepting a message addressed to the PIN entry device, for generating the third message from the first message and a user-entered PIN, for encrypting the third message according to an encryption key stored in the memory of the token and for transmitting the third message to the token.